LiveAction®

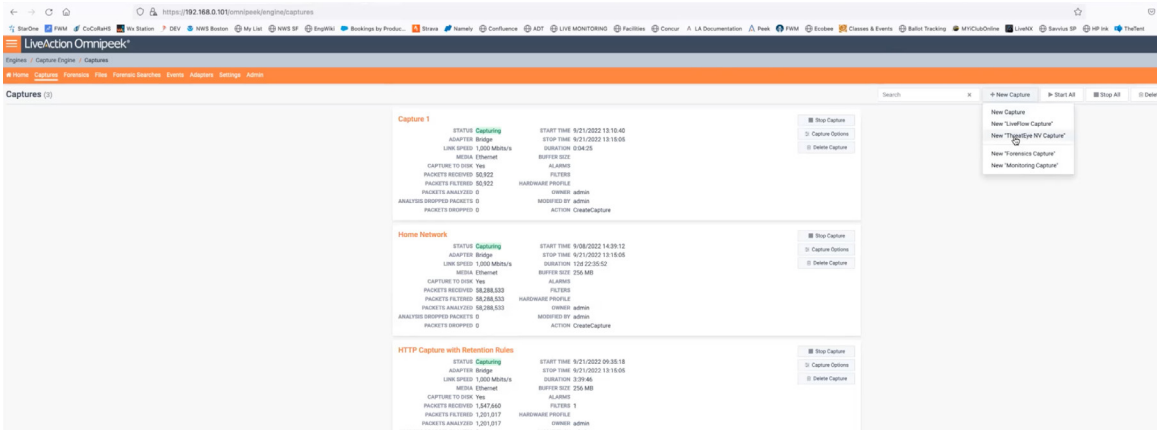
ThreatEye

How-To Guide: ThreatEye Capture

How to Apply ThreatEye Capture

How to Apply ThreatEye Capture

Within the " + New Capture" area there's something called "New ThreatEye Capture"

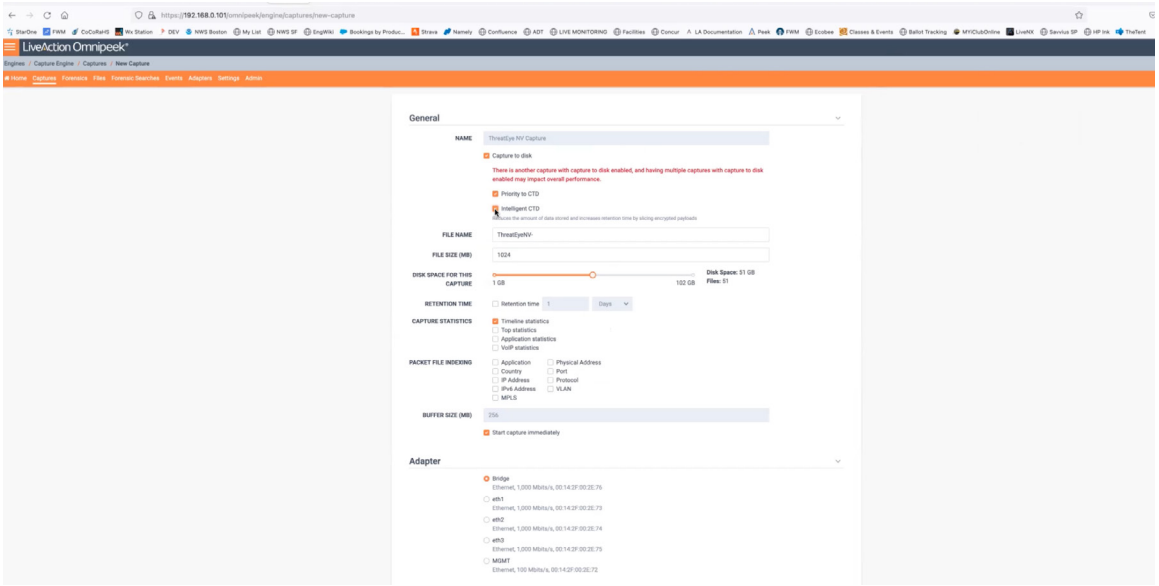


This view has many of the same options as a new capture, but there are also preconfigured settings that are in place.

A ThreatEye customer today who's using LiveWire to generate the data will use this page to start that dataflow.

PLEASE NOTE: Currently, packet capture is visible and available for ThreatEye customers as a free license in addition to their ThreatEye Capture product. This is something subject to change in the future that may require an add-on fee or a separate license.

Users can enter the captures from their home page and select the "New ThreatEye Capture".



ThreatEye scans every packet for indicators of threats and generates data about each packet.
If you turn on "Capture to Disk," the first checkbox, it writes the packet to a file for storage.

Why store packets?

It allows you to review data collected over time and if issues arise, audit the network traffic, click a button in the ThreatEye user interface, and link back directly into the packet file.

The benefit of combining Intelligent Packet Capture with ThreatEye Capture

The major benefit to IPC is increased data storage space, encrypted traffic is not accessible to most users without the correct decryption keys. For example, if it's traffic between a desktop and Salesforce the end user is not going to have the private part of the key from Salesforce to the encrypted traffic.

It takes up valuable space. If you can slice off the payloads from data, there is more room for packet headers and longer storage times.

Adding ThreatEye can ensure that the encrypted payload being discarded do not contain malicious code.

Use cases for unchecking Intelligent Packet Capture (IPC) Feature

Customers may have their own web applications they know the keys to so they can go back and decrypt the data. In those cases, they might not want to slice off the encrypted part of the packet, if they really wanted to go back and interrogate it, they could take their keys and put them into the software, and we would then decrypt that flow.

If a customer wanted to use IPC and slice some traffic but not all their traffic and retain some encrypted traffic, they can start several of these captures by selecting specific characteristics.

You can select a filter for only web traffic to be excluded from IPC, and have a second one running that's all other traffic with IPC selected.

Capture Limitations

There is no theoretical or programmatic limit to the number of captures, but there are practical limits. Starting another capture does not double your ability to capture at a higher rate. The rate is fixed, so adding multiple characteristics splits up the capabilities and can affect throughput.

We only allow one live flow capture and one ThreatEye capture at once, although you can start as many other generic captures as you want